

AMENDMENTS TO THE DRAWINGS

The only figure has been labeled FIG. 1

Attachment: One (1) Replacement Sheet

REMARKS

Claims 1-6, 8 and 9 are all the claims pending in the application. By this Amendment, Applicant amends claims 1 and 6 to further clarify the invention.

I. Summary of the Office Action

The Examiner objected to the drawings for a minor informality and maintained the rejections of claims 1-9 under 35 U.S.C. § 103(a).

II. Objection to the Drawings

The Examiner has objected to the drawings for failing to label the only figure, FIG. 1. Applicant has amended the drawing to remedy this minor informality. A replacement drawing accompanies this response. Accordingly, Applicant respectfully requests the Examiner to withdraw this objection to the drawing. For conformity therewith, Applicant amends the specification to refer to the drawing as FIG. 1. No new matter is being added.

III. Prior Art Rejections

Claims 1-4 and 6-8 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,526,418 to Midgley et al. (hereinafter “Midgley”), in view of U.S. Patent No. 7,093,135 to Radatti et al. (hereinafter “Radatti”) and claims 5 and 9 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Midgley and Radatti, in view of U.S. Patent No. 5,799,323 to Mosher, Jr. (hereinafter “Mosher”). Applicant respectfully traverses these grounds of rejection at least in view of the following exemplary comments.

Of these rejected claims, only claims 1 and 6 are independent. These independent claims in some variation *inter alia* recite; wherein receipt of any data from the data communications network is limited to the first computer; wherein transmission of any data to the data

communications network is limited to the second computer; wherein the first computer is configured to convert, transmit to and store in the second computer non-verified or non-verifiable data received by the first computer only in non-processable form.

In an exemplary, non-limiting embodiment, the computer system has two parallel computers, which have practically the same hardware structure and which are configured with the same software. To achieve the required security, receiving any data from the data communications network and at least the initial processing of the received data is limited to the first computer, while transmitting any data to the data communications network is limited to the second computer. This can be achieved by a hardware or software transmission block or reception block, respectively. In other words, all of the data is received by the first computer, whereas the second computer transmits all of the data.

In addition, in the context of the initial processing of the received data, which is limited to the first computer, the received data can be verified. Therein, the second computer can accept and store only verified data in unlocked, i.e., processable form. Unverified or non-verifiable data received by the first computer is accepted by the second computer only in locked (encapsulated), i.e., non-processable form. The locked data can neither be opened nor processed in the second computer but can only be transmitted by the second computer since the first computer cannot transmit this data. In other words, the first computer converts data into a locked state if the data cannot be verified.

Accordingly, the second, redundant computer, which is prevented by hardware or software means from receiving data from the data communications network, remains free from computer viruses. In addition, no computer viruses can be transmitted to the outside world when data is being sent nor can data be fetched or corrupted by so-called Trojan horses. If the first

computer is infected with computer viruses because of data received from the data communications network, then this infection is immediately detected when the two computers are matched. In this case, the first computer can be restored to a virus-free state by copying the state of the second computer onto the first computer, without any data or previously performed work being lost.

It will be appreciated that the foregoing remarks relate to the invention in a general sense, the remarks are not necessarily limitative of any claims and are intended only to help the Examiner better understand the distinguishing aspects of the claims mentioned above.

In response to Applicant's arguments that the prior art of record do not disclose or suggest the unique features of claims 1 and 6, the Examiner alleges that a) col. 12, line 53 to col. 13, line 16 of Midgley disclose having a first computer that is limited to receiving data and having a second computer that is limited to transmission of data as set forth in claims 1 and 6 and b) col. 7, lines 10 to 35 of Radatti discloses transmitting and storing data in a non processable format when the data is unverifiable as set forth in claims 1 and 6 (*see* pages 2-3 of the Office Action). Applicant respectfully disagrees.

Col. 12, line 53 to col. 13, line 16 of Midgley recites:

Once the data source files have been identified by the user, the process backup system may employ the synchronization replication process 40 to create a replicated image of the selected data source files at the back up server 12. In one process, the backup system may first begin by creating copies of the data source files and storing them as replicated files on the back up server 12. Thus, to synchronize the data on the source and backup systems, the backup system can begin by making a copy of each source data file and storing it as a target data file on the backup server system and, optionally, writing the target data file to long term storage, such as to a tape storage media. If a file is closed, the back up system may compare the source files metadata and, may compare its contents. If the file is open, the backup system may compare the file contents. To synchronize [sic] the source data files and the target data files, the backup system replicates the changed data to the backup storage device

and writes the changed data to the storage target. The change can be committed when that change is written to the storage target. As the copying of thousands of files may take time, the source data files may change during the copying process. To address this, the dynamic replication process will execute and capture file modifications to the source files being synchronized and journal them to the backup server. Once the synchronization replication process has finished processing an individual source file or a transactional group of files, the dynamic execution process may play the captured changes to the target file(s). This ensures the target file(s) are updated in a transactionally safe way, and keeps the target files as up to date as possible while still keeping them transactionally safe.

As is visible, the above quoted passage of Midgley simply discloses data replication to the backup server. However, Midgley clearly fails to disclose the division of incoming and outgoing data on different computers in that any receipt of data is limited to the first computer and that any transmission of data is limited to the second computer. In Midgley, both the servers 18 to 22 and the backup server 12 must be able to both receive and send at least some of the data in order to save data from a server 18 to 20 in the backup sever 12 and to later retrieve that data from the backup server 12 (Fig. 1). In short, Midgley reference fails to disclose that receipt of any data from the data communications network is limited to the first computer and transmission of any data to the data communications network is limited to the second computer. In Midgley, there is no disclosure or suggestion that the first and second computers are limited to these functions. Radatti does not cure the above-identified deficiencies of Midgley.

Furthermore, col. 7, lines 10 to 35 of Radatti recites:

When a Document with Macros is Opened AutoMacros, such as AutoOpen, are not allowed to run. Macros are checked for validation key. If a key is present, the hash code for the macro is compared to the macro to insure the macro is unchanged. If the macro has no key, a copy is made of the document, the copy may be optionally retained in a buffer, and the original is sent to the validation component for authentication. Any subsequent dissemination of the document will then be from the original after validation. Otherwise, if the copy is infected and is disseminated, any recipient will be infected as well. If an Encrypted or Unencrypted Macro does not Match its Hash Code

A system administrator will be alerted.

The macro will not be permitted to run.

Of course, other configurations for the workstation are possible. For example, the user's access to macros can be limited in a number of ways: such as prohibiting a user from deleting or editing validated macros; prohibiting all macros from running; etc. A user might be alerted to the presence of a validated or unvalidated macro and any alerts that might be provided could be specific in nature. For example, in an embodiment, a desired alert might be something like "Virus Detected, call Veronica at X1234 for help.

As is visible, the above quoted passage of Radatti simply discloses prohibiting macros from running when their hash code does not match. Radatti, however, does not disclose or suggest that this non-verified or non-verifiable data is first received by a first computer and then transmitted to and stored in a second computer in non-processable form. In other words, Radatti does not disclose or even remotely suggest the first computer converting the data into a non-processable form for a transmission to the second computer. Radatti simply discloses the user being prevented from running the macro and not that it is converted into non-processable form for transmission to a different computer.

For at least these exemplary reasons, claims 1 and 6 are patentable over the prior art of record. Claims 2-4 and 8 are patentable at least by virtue of their dependency on claims 1 and 6, respectively.

Claims 5 and 9 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Midgley and Radatti in view of Mosher. Applicant respectfully traverses these grounds of rejection at least in view of the following exemplary comments.

Claims 5 and 9 depend on claims 1 and 6, respectively. Applicant has already demonstrated that Midgley and Radatti do not meet all the requirements of independent claims 1

and 6. Mosher does not compensate for the above-identified deficiencies of Midgley and Radatti. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of claims 1 and 6. Since claims 5 and 9 depend on claims 1 and 6, respectively, they are patentable at least by virtue of their dependency.

IV. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/Nataliya Dvorson/
Nataliya Dvorson
Registration No. 56,616

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: January 15, 2008